Industrial Security Program & DD Form 254, Contract Security Classification Specification Implementation Guide

Definitions | Chapter 1 | Chapter 2 | Appendix A | Appendix B | Appendix C
Appendix D | Appendix E | Appendix F | Appendix G | Appendix H

FORWORD

This guide provides preparation instructions for DD Form 254, Contract Security Classification Specification, and should be used in conjunction with DOD 5220.22-R, Industrial Security Regulation (ISR), and DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM). It applies to contracting and procurement officials, program and project managers. All share functional industrial security program responsibilities within the Defense Information Systems Agency/Office of the Manager, National Communications System (DISA/OMNCS).

The DD Form 254 is a key document in contracting actions. The form, with its attachments, supplements and incorporated references, advises contractors on the proper procedures to handle classified material received or generated under a classified contract. It identifies which security classification guidance to use, who has oversight, and where. The DD Form 254 should be kept unclassified, if at all possible. If you need to supply classified guidance, transmit it under separate cover by an approved method of transmission.

For more information, contact the DISA/OMNCS Industrial Security Program Manager at Commercial (703) 681-1350 or
DSN 761-1350.

ROBERT W. ROGALSKI

Chief of Security

REFERENCES

a. DOD 5220.22-R, Industrial Security Regulation, December 1985

b. DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), January 1995

c. DOD 5220.22-M-Sup 1, National Industrial Security Program Operating Manual Supplement, February 1995

d. DOD 5220.22-S-1, COMSEC Supplement to the Industrial Security Regulation, August 1983

e. DOD 5200.1-R, Information Security Program, January 1997

f. DOD 5200.2-R, Personnel Security Program, January 1987

g. DOD Instruction 5230.24, Distribution Statements on Technical Documents, 18 March 1987

h. DOD Directive 5205.2, DOD Operations Security (OPSEC) Program, 7 July 1983

i. DIAM 50-4, Security of Compartmented Computer Operations (U), 24 June 1980

j. DIAM 50-5, Volumes I & II, Sensitive Compartmented Information (SCI) Contractor Administrative Security, 22 October 1979

k. Director of Central Intelligence Directive (DCID) 1/7, Security Controls on the Dissemination of Intelligence Information, 12 April 1995

l. DCID 1/14, Minimum Personnel Security Standards and Procedures Governing Eligibility for Access to SCI,
22 January 1992

m. DCID 1/19, Security Policy for SCI (U), 28 June 1982

n. DCID 1/21, Physical Security Standards for SCI, 28 June 1994

o. DOD 5200.28-STD, DOD Trusted Computer System Evaluation Criteria, 26 December 1995

DEFINITIONS

ACCESS: The ability and opportunity to obtain knowledge of classified information.

ACCESSES: Indoctrination to classified material that has additional security requirements or caveats. This may be Sensitive Compartmented Information (SCI), Special Access Program (SAP) information, or collateral level accesses such as North Atlantic Treaty Organization (NATO), Critical Nuclear Weapons Design Information (CNWDI), etc.

CLASSIFIED CONTRACT: Any contract that requires or will require access to classified information, by a contractor or his or her employees. (A contract may be a classified contract even though the contract document is not classified.) The requirements for a classified contract also are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other Government Contracting Agency programs or projects, which require access to classified information by a contractor.

COGNIZANT SECURITY AGENCY (CSA): Agencies of the Executive Branch that have been authorized by Executive Order (E.O.) 12829 to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of those agencies when disclosed or released to industry. Denotes the Department of Defense, the Department of Energy, the Nuclear Regulatory Commission, and the Central Intelligence Agency. The Secretary of Defense, the Secretary of Energy, the Director of Central Intelligence and the Chairman, Nuclear Regulatory Commission may delegate any aspect of security administration regarding classified activities and contracts under their purview within the CSA or to another CSA. Responsibility for security administration may be further delegated by a CSA to one or more Cognizant

Security Offices (CSOs). For contractors participating in the National Industrial Security Program (NISP), the CSA is the Department of Defense.

COGNIZANT SECURITY OFFICE (CSO): The CSO is always the Defense Investigative Service, Director of Industrial Security, who has jurisdiction over the geographical area in which the contractor is located. If someone will conduct inspections other than the CSO, DIS must be relieved in the DD Form 254, by completing Item
15 as appropriate. Inspections by an Agency other than DIS do not affect the CSO designation and do not relieve the contracting activity from the responsibility of providing a copy of the DD Form 254 to the CSO.

CONTRACTING OFFICER: A Government official, who in accordance with departmental or agency procedures, currently is designated as a contracting officer with the authority to enter into and administer contracts, and make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representative of the contracting officer acting within the limits of his or her authority.

CONTRACTOR: Any industrial, educational, commercial, or other entity that has been granted a Facility Security Clearance (FCL) by a CSA.

ENTRANCE NATIONAL AGENCY CHECK (ENTNAC): A personnel security investigation scoped and conducted in the same manner as a National Agency Check (NAC) except that a technical fingerprint search of the files of the Federal Bureau of Investigation (FBI) is not conducted.

FACILITY (SECURITY) CLEARANCE (FCL): An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

INTERIM SECURITY CLEARANCE: A security clearance based on the completion of minimum investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

MEMORANDUM OF AGREEMENT (MOA): A formal agreement between or among agencies or activities to delineate specific functions.

NATIONAL AGENCY CHECK (NAC). A personnel security investigation consisting of a records review of certain agencies as described in paragraph 1, Appendix B, of DOD 5200.2-R, Personnel Security Program Regulation (Enclosure 5), including a technical fingerprint search of the files of the FBI.

NATIONAL AGENCY CHECK PLUS WRITTEN IQUIRIES (NACI): A personnel security investigation conducted by the Office of Personnel Management, combining a NAC and written inquiries to law enforcement agencies, former employers and supervisors, references, and schools.

OWNERSHIP OF CLASSIFIED INFORMATION: Once information is determined to be classified, it belongs to the United States Government and not the contractor, regardless of proprietary claims.

PERSONNEL (SECURITY) CLEARANCE (PCL): An administrative determination that an individual is eligible, from a security viewpoint, for access to classified information at the same or lower category as the level of the personnel clearance being granted.

SENSITIVE COMPARTMENTED INFORMATION (SCI): Information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

SINGLE SCOPE BACKGROUND IVESTIGATION (SSBI). A personnel security investigation consisting of both record reviews and interviews with sources of information prescribed in paragraph 3, Appendix B, DOD 5200.2, Personnel Security Program Regulation (Reference a), plus certain additional investigative requirements as prescribed in paragraph 4, Appendix B, DOD 5200.2-R (Reference a). The period of investigation for an SSBI is the last 10 years or since the 18th birthday, whichever is shorter, provided the last 2 full years are covered and that no investigation will be conducted prior to an individual’s 16th birthday.

SPECIAL ACCESS PROGRAM (SAP): Any program approved in accordance with DOD 5200.1-R, Chapter VIII, which imposes need-to-know access controls beyond those normally required for access to collateral (TOP SECRET, SECRET, and CONFIDENTIAL) information.

CHAPTER 1

1.1 Background.

1.1.1 Executive Order 12829, National Industrial Security

Program, establishes the National Industrial Security Program. DOD 5220.22-M, National Industrial Security Operating Manual (NISPOM), DOD 5220.22-R, Industrial Security Regulation (ISR), and DOD 5220-22.M-Supplement 1, National Industrial Security Program Operating Manual Supplement (NISPOMSUP), implement NISP requirements. This NISPOM establishes uniform security policies, practices, and procedures to ensure the proper safeguarding of classified information throughout industry.

1.1.2 The NISPOM implements applicable Federal statutes, Executive Orders, and national directives.

1.1.3 The NISPOM prescribes requirements, restrictions and other safeguards that are necessary to prevent the unauthorized disclosure of classified information and to control authorized disclosure of classified information by the United States Government Executive Branch Departments and Agencies and their contractors. The NISPOM replaces DOD 5220.22-M, Defense Industrial Security Manual for Safeguarding Classified Information, January 1991.

1.1.4 The NISPOMSUP prescribes special security measures to ensure the integrity of Special Access Programs (SAPs), Restricted Data (RD), and Sensitive Compartmented Information (SCI), and imposes supplemental controls to those requirements prescribed in the NISPOM.

1.2 Introduction.

1.2.1 Early in the acquisition cycle, certain security requirements must be considered. Will access to classified information be involved? Will access be required during the pre-award phase, or will it only be required for actual performance of the contract? Are all the prospective contractors cleared to the appropriate level, and are they equipped to properly safeguard the classified information involved? The answers to these questions and the timeliness of your actions will have a significant impact on your acquisition and the National Industrial Security Program (NISP).

1.2.2 As a part of the provided contracting process, enough lead-time should be in your acquisition cycle to accomplish the security actions that may be needed. In many instances, advanced planning can ensure that the bid package will not require access to classified information, which precludes processing an entire bidders list for a facility security clearance. When access is required in the pre-award phase, an interim facility security clearance (FCL) may be the solution. If access is not a factor in the pre-award phase, but will be required for contract performance, only the successful bidder will be processed for an FCL. Unnecessary processing of prospective contractors for FCLs is time consuming, costly and increases the time it takes to process a contractor who actually has a need for an FCL.

1.2.3 A Contract Security Classification Specification, DD Form 254, is required for each classified contract and must be incorporated in the solicitation and in the contract. Even if pre-award access is not required, the DD Form 254 must be incorporated in the solicitation to allow the contractor the information needed for performance. In this event, add the following statement in Item 13 of the DD Form 254:

"Pre-award access is not required. This DD Form 254 reflects the security requirements for the contract when awarded."

1.2.4 A review of security requirements should be performed at the various stages of acquisition; pre-award, award, research and development, production, etc., and if required, a revised DD Form 254 must be issued. However, you must review the DD Form 254 at least biennially, and forward to the contracting officer (KO), DISA Security Programs and Oversight Branch (D161), and the CSO, either the updated DD Form 254, or a letter, identifying the contract and contractor, stating the DD Form 254 has not changed. On final delivery of goods or services, or on completion or termination of the contract, the contractor is required to return to the User Agency (UA) or Contracting Officer’s Representative (COR) all classified material received or generated under the contract, or to destroy all classified material unless retention is requested for a specific period of time and authorized in writing by the KO. As the COR, you must have knowledge of all classified material received or generated by the contractor under your contract.

1.2.5 The DD Form 254, with its attachments and incorporated references, is the only authorized means for providing security classification guidance to the contractor. Security classification guidance should be written as specifically as possible and should include only information that pertains to the specific contract. Any and all documents referenced in a DD Form 254 should be provided to the contractor, either as an attachment or forwarded under a separate cover, if they are classified. The requirements of DOD 5220.22-M, NISPOM, should not be included in a DD Form 254; the NISPOM contains the specific safeguarding and procedural requirements for the contractor, not security classification guidance.

1.2.6 Classified Information (TOP SECRET, SECRET, and CONFIDENTIAL), is, and remains for the duration of the classification, the property of the U.S. Government, regardless of proprietary claims. It may be provided to private industry only in connection with a bona fide contractual requirement. Prior to a contractor having access to classified information, a Security Agreement, DD Form 441, is executed between the Government and the contractor. This agreement requires the contractor to protect classified information in accordance with the requirements of the NISPOM, and it obligates the Government to specifically identify, in writing, what information will require protection during the contract performance. The NISPOM provides the contractor the minimum safeguarding requirements for classified information; it does not provide security classification guidance (SCG). The SCG is provided in the body of the DD Form 254 (Figure 1) or its attachments. The DD Form 254 with its attachments, supplements, and incorporated references, is the only authorized means for providing SCG to a contractor in connection with a

classified contract. The following information provides an explanation of the various items on the DD Form 254 to assist in its preparation.

1.3 Suitability Determinations.

1.3.1 Contractor personnel performing on DISA/OMNCS contracts who are assigned duties using sensitive unclassified automated information systems (AISs) designated as ADP-I, ADP-II, or ADP-III in accordance with reference 4.5, must be the subject of an investigation to determine the individual’s suitability to occupy the position. NOTE: The background investigation requirement is not applicable when the contractor employee has a valid PCL at or above the ADP designation investigation level on file with the Defense Investigative Service Clearance Office (DISCO).

1.3.2 The Standard Form (SF) 85P, Questionnaire for Public Trust Position, must be completed and submitted to the Security Division (D16), Personnel Security Office (D162), for the appropriate scope and background investigation to be conducted.

1.3.3 Once the investigation is completed, the results are returned to the Personnel Security Office (D162), where the suitability determination is made.

CHAPTER 2

SECTION 1. GENERAL INSTRUCTIONS:

2.1.1 Introduction.

This section contains instruction for preparation of the "Contract Security Classification Specification" (DD Form 254) for classified contracts. The DD Form 254, with its attachments, supplements, and incorporated references is designed to provide a contractor with the security requirements and classification guidance needed for performance of the classified contract. However, there are many actions required by the contracting activity in preparation of the DD Form 254. For example, when a contractor requires access to certain types of classified information, the contracting activity must ensure that the contractor has the special procedures in place to safeguard those types of information. You must verify this information by contacting the Defense Investigative Service/Central Verification Activity (DIS/CVA), at Commercial (410) 865-2720, or by requesting the CSO to establish the procedures at the contractor’s facility. The DD Form 254 is not the vehicle for requesting the CSO to establish such procedures; the contracting activity must provide the CSO with written justification for such procedures. The contracting activity is responsible for ensuring that proper security

procedures are in place at the contractor facility prior to releasing any classified information to a contractor.

2.1.2 Safeguarding Verification.

If the contract calls for access to COMSEC, Restricted Data (RD), Formerly Restricted Data (FRD), Critical Nuclear Weapons Design Information (CNWDI), NATO, or foreign government information, you must ask the DIS/CVA computer operator if the contractor company has access to this type of information; it will not be volunteered.

2.1.3 Preparing the DD Form 254.

The following information corresponds to the items on the DD Form 254. An explanation, as well as other pertinent information, is provided for each item on the DD Form 254. This guide covers general circumstances. If the contract has specific requirements, tailor it to fit your needs. If you have questions about the DD Form 254, call the DISA Security Division (D16).

SECTION 2 - PREPARATION INSTRUCTIONS

2.2.1 ITEM 1, CLEARANCE AND SAFEGUARDING:

2.2.1.1 In Item 1a, insert the highest level of FCL required by the contractor for performance of the contract. Use only the words TOP SECRET, SECRET or CONFIDENTIAL. Special caveats, such as RESTRICTED DATA (RD), FORMERLY RESTRICTED DATA (FRD), etc., are not appropriate in this item. The contractor must have a valid FCL at least as high as the classification indicated in this item (verify the contractor’s FCL with DIS/CVA if this information is not known).

2.2.1.2 In Item 1b, insert the highest level of safeguarding capability required by the contractor for performance of the contract.

2.2.1.3 The classification level shown in 1b may not be higher than that shown in Item 1a. If the contractor will not possess classified information at the cleared facility in performing the contract, enter Not Applicable (N/A) or None.

2.2.2.1 ITEM 2, THIS SPECIFICATION IS FOR:

Insert "X" in Item 2a for a prime contract and enter the contract number and expiration date. Insert "X" in Item 2c for a solicitation (Request for

Proposal (RFP), Request for Quotation (RFQ), Invitation for Bid (IFB), or other UA program or project) and enter an appropriate identification number. Enter due date for a solicitation as appropriate. Item 2b is for use by contractors for their subcontractors.

2.2.3.1 ITEM 3, THIS SPECIFICATION IS:

When the original DD Form 254 is issued, insert "X" in Item 3a and enter date. The date of the original will appear unchanged on each revised or final DD Form 254 issued thereafter. Item 3a applies when a solicitation is issued and when the contract is awarded. When a revised DD Form 254 is issued, insert "X" in Item 3b, show revision number, and enter date of revision. Each time a revision is issued, it shall be given a sequential revision number. When a final DD Form 254 is issued, insert "X" in Item 3c and enter date. When Item 3c is "Yes," Item 5 is "Yes." A final DD Form 254 is not required unless the contractor requests an extension of retention authority and the KO authorizes approval.

2.2.3.1.1 The program/project manager or other official of the U.S. (COR) who prepared the original, final, or revised DD Form 254, reviews the form at least biennially. Refer to DOD 5220.22-R, Industrial Security Regulation, paragraph 7-104, for additional information and exceptions.

2.2.3.1.2 Contractors shall return or destroy classified material in accordance with the following schedule:

2.2.3.1.2.1 If a bid, proposal, or quote is not submitted or is withdrawn, within 180 days after the opening date of bids, proposals, or quotes.

2.2.3.1.2.2 If a bid, proposal, or quote is not accepted, within 180 days after notification that a bid, proposal, or quote is not accepted.

2.2.3.1.2.3 If the successful bidder, within 2 years after final delivery of goods and services; or, after completion or termination of the classified contract, whichever comes first.

2.2.3.1.2.4 If the classified material was not received under a specific contract, such as material obtained at classified meetings or from a secondary distribution center, within 1 year after receipt.

2.2.3.1.3 Contractors may retain classified material up to 2 years after the completion or termination of the contract (if not advised to the contrary by the contracting office) without applying for retention authority. Contractors

desiring to retain classified material received or generated under a contract beyond the 2-year period must request and receive written retention authority from the contracting office.

2.2.4 ITEM 4, IS THIS A FOLLOW-ON CONTRACT?:

This item pertains to follow-on contracts only. The contract must be to the same contractor for the same item or service as the preceding contract. When these conditions exist, enter "X" in the "Yes" box, and enter the preceding contract number in the space provided. This item authorizes the contractor to transfer classified material received or generated under the preceding contract to the current contract. The need for the contractor to notify the UA of retention is eliminated until completion of the follow-on contract. It is assumed that the contractor will require access to the same information for performance of the follow-on contract as was required for the preceding contract. If this is not a follow-on contract, enter "X" in the "No" box.

2.2.5 ITEM 5, IS THIS A FINAL DD FORM 254?:

If a final DD Form 254 is being issued, enter an "X" in the "Yes" box, the date of the contractor’s retention, and the authorized period of retention in the spaces provided. If this is not a final DD Form 254, enter "X" in the "No" box. (Also see Item 3 description, last paragraph).

2.2.6 ITEM 6, CONTRACTOR:

Enter the name and address of the prime contractor in Item 6a. Enter the Commercial and Government Entity (CAGE) code in Item 6b, and the name and address of the CSO in Item 6c. The appropriate CSO can be found in Appendices "F" and "G" of this handbook.

2.2.7 ITEM 7, SUBCONTRACTOR:

The prime contractor completes this item when subcontracting.

2.2.8 ITEM 8, ACTUAL PERFORMANCE:

If work is to be performed at a location (of the company) other than specified in 6a, enter the appropriate name and address in Item 8a, the CAGE code in Item 8b, and name and address of the CSO in 8c. DIS will provide the CAGE code at the time of FCL verification if you do not have it. The CSO is always the

DIS, Director of Industrial Security, who has jurisdiction over the geographical area in which the contractor is located. No other activity should be shown in this block. Inspections conducted by an UA other than DIS do not affect the CSO designation and do not relieve the contracting activity from the responsibility of providing a copy of the DD Form 254 to the CSO. If someone will conduct an inspection other than the CSO, or if DIS will be relieved of security cognizance, complete Item 15 as appropriate.

2.2.9 ITEM 9, GENERAL IDENTIFICATION OF THIS PROCUREMENT:

Enter a short, concise, and unclassified description of the procurement action (i.e., research, development, production, study, services, etc.) in Item 9.

2.2.10 ITEM 10, THIS CONTRACT WILL REQUIRE ACCESS TO:

Mark these items "Yes" or "No" according to the requirements of each contract.

2.2.10.1 ITEM 10a, COMSEC:

If the contractor requires access to any COMSEC information, enter "X" in the "Yes" box. COMSEC information includes accountable and/or non-accountable COMSEC information and Controlled Cryptographic Items (CCI). If accountable COMSEC
information is involved, the contractor must have a COMSEC account and Item 11h would be marked "Yes." If Item 10a is "Yes," then add:

"Reference Item 10a: Contractor is authorized to receive Government furnished cryptographic equipment. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level. Further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior approval of the contracting activity."

2.2.10.2 ITEM 10b, RESTRICTED DATA:

This item is marked "Yes" if access to information that is classified and controlled under the Atomic Energy Act of 1954 is required. This item is marked "Yes" if Item 10c is marked "Yes."

2.2.10.3 ITEM 10c, CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI):

This item will be marked "Yes" if access to CNWDI is required. Permission of the contracting activity is required prior to subcontracting CNWDI. Special briefings and procedures are also required. A Government representative initially briefs the contractor Facility Security Officer (FSO) for CNWDI, who, in turn, briefs other contractor employees. Insert the following statement in Item 13: "Reference Item 10c: This contractor is permitted access to CNWDI in performance of the contract. The Government program manager or designated representative ensures the contractor security supervisor is briefed for access to CNWDI by a Government representative prior to granting access."

2.2.10.4 ITEM 10d, FORMERLY RESTRICTED DATA:

Mark this "Yes" if access to FRD is required.

2.2.10.5 ITEM 10e, INTELLIGENCE INFORMATION:

This is information under the jurisdiction and control of the Director of Central Intelligence (DCI) and circulated within the intelligence community. If intelligence information is involved, the contracting activity is responsible for ensuring that the additional security requirements outlined in Director, Central Intelligence Directives (DCIDs) 1/7 and 1/21, and Defense Intelligence Agency Manuals (DIAMs) 50-4 and 50-5, are incorporated in the guidance provided to the contractor and is tailored to the performance of the contract. The guidance may be included in the contract document itself or Item 13. The CSO does not conduct inspections for Sensitive Compartmented Information (SCI), but must inspect non-SCI intelligence material the contractor possesses.If access to SCI is required, mark Items 10e(1), 14, and 15 "Yes."

2.2.10.5.1 If access to non-SCI Intelligence information is required, mark Item 10e(2) "Yes." Item 14 would also be marked "Yes," and Item 15 would be marked "No." The CSO (DIS) is responsible for inspections of non-SCI intelligence information in the possession of a contractor.

2.2.10.5.3 NOTE: Prior approval of the contracting activity, to include coordination with the CSA, is required for subcontracting. The contractor or contract monitor must have SCI indoctrinated personnel available to work the contract. Officially request the SCI billets required for the contract from DISA Security Division (D16), Special Security Office (SSO) via Interoffice Memorandum. The contract document and DD Form 254 must have the security clauses required by DIAMs 50-4 and 50-5, and DCID 1/21. They provide the necessary guidance for physical, personnel, information, classification, and TEMPEST security measures and are part of the SCI security specifications for the contract. Item 1 must read TOP SECRET.

2.2.10.6 ITEM 10e(1), SENSITIVE COMPARTMENTED INFORMATION (SCI):

2.2.10.6.1 When Item 10e(1) is "Yes," include the following statement in Item 13:

"Reference Item 10e(1): This contract requires access to SCI.

a. The Director, Defense Intelligence Agency (DIA) and Director, DISA, as the executive agents for DIA, have exclusive security responsibility for SCI released to the contractor or developed under this contract.

b. Contractor generated or Government furnished material may not be provided to the Defense Technical Information Center (DTIC). Contract generated technical reports will bear the statement Not Releasable to the Defense Technical Information Center per DOD Instruction 5230.24.’

c. All contractor personnel requiring access to SCI information must: be U.S. citizens, have been granted a final Top Secret security clearance by the U.S. Government, have been approved as meeting DCID 1/14 criteria by a Government Cognizant Security Agency, and have been indoctrinated for the applicable compartments of SCI access prior to being given any access to such information released or generated under this contract. Immigrant aliens, personnel cleared on an interim basis, or personnel holding contractor granted CONFIDENTIAL clearances, are
not eligible for access to classified information released or generated under this contract without the expressed permission of the Director, DISA (through the DISA Security Division SSO (D162)) and the Director, DIA.

d. Classified material released or generated under this contract is not releasable to foreign nationals without the expressed written permission of the Director, DISA (SSO) and Director, DIA.

e. Recipients of SCI under this contract may not be released to subcontractors without permission of the DISA SSO.

f. STU-III terminals installed at the contractor’s facilities shall be supported by a COMSEC account (of the contractor of DISA). STU-IIIs in SCI Facilities (SCIFs) require Class VI Cryptographic Ignition Key (CIK).

g. The contractor and COR will revalidate all SCI billets under this contract with the DISA Security Operations Division (D162) annually or when a revised DD Form 254 issued, whichever is sooner."

2.2.10.6.2 If Item 10e(1) is "Yes," Items 12, 14 and 15 will be "Yes" with the following statements added:

2.2.10.6.2.1 In Item 12, "Public release of SCI/SAP material is not authorized."

2.2.10.6.2.2 In Item 14, "The contractor will abide by DIAMs 50-4 and 50-5, Volumes I and II, and DCID 1/21."

2.2.10.6.2.3 In Item 15, "The DISA Security Division (D16) will be responsible for inspection of SCI under this contract."

2.2.10.6.3 If Item 10e(1) and 11a are "Yes," then Items 11b and c are "No," and the following statement must be included in Item 13:

"Reference Items 10e(1) and 11a: All contractor SCI work and access will be at a designated Government approved SCI Facility (SCIF)."

NOTE: The COR will coordinate with the DISA Security Division (D16) to identify the SCIF and initiate any Memorandums of Agreement (MOAs) as required.

2.2.10.7 Item 10e(2), NON-SCI INTELLIGENCE INFORMATION:

This item will be marked "Yes," only if access is required to the material marked: (1) DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR (ORCON), or (2) AUTHORIZED FOR RELEASE TO: (Name of Country(ies), or international organizations).

2.2.10.7.1 The control markings, "Warning Notice - Intelligence Sources or Methods Involved," "Not Releasable to Contractors or Consultants," and "NOFORN" are no longer authorized for use. The markings "WNINTEL," "NOCONTRACT," or "NOFORN" will not be used on any newly created documents or other materials. For automated information systems, a phase-in elimination of these markings will be accomplished as systems are upgraded or software is modified, but not later than 12 April 2000. Remarking of the material bearing the "WNINTEL," "NOCONTRACT," and "NOFORN" control markings is not required. However, holders of material bearing these markings may line through or otherwise remove the markings from the documents or other material. The presence of these markings, in themselves, will have no bearing on the ability to release it to contractors.

2.2.10.7.2 Other obsolete markings include: WARNING NOTICE- SENSITIVE SOURCES AND METHODS INVOLVED; WARNING NOTICE-INTELLIGENCE SOURCES AND METHODS INVOLVED; WARNING NOTICE-SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED; CONTROLLED DISEM, NSC PARTICIPATING AGENCIES ONLY; INTEL COMPONENTS ONLY; LIMITED, CONTINUED CONTROL; NO DISSEM ABROAD; BACKGROUND USE ONLY; USIB ONLY; NFIB ONLY; and NOT RELEASABLE TO FOREIGN NATIONALS.

2.2.10.8 ITEM 10f, SPECIAL ACCESS INFORMATION:

This means a Special Access Program (SAP) or code word that has been approved by the head of a UA (reference: DOD Directive O-5207.5). When this Item is marked "Yes," the contracting activity is responsible for providing the contractor with the additional security requirements needed to supplement the NISPOM requirements and ensure adequate protection of the SAP information involved. They may be included in the contract document itself, but will be referenced in Item 13. Item 14 will be marked "Yes," and Item 15 will be completed as appropriate. Prior approval from the contracting activity is required, including coordination with the DISA Security Division (D16) prior to subcontracting. Access to SAP information requires a final U.S. Government clearance at the appropriate level
identified in the SAP Security plan/directives. All DD Forms 254 requiring SAP access will be coordinated with and processed through the DISA Security Division (D16).

2.2.10.8.1 If Item 10f is "Yes," include the following statement: "Reference Item 10f: To execute this contract, additional security requirements in addition to DOD 5220.22-M will be required. The contractor shall comply with the security provisions of these programs. Marking and/or classification guidance for material originated or generated under this contract will be provided through the DISA Security Operations Division (D162) under separate cover. Any material generated by the contractor (including correspondence, drawings, models, mockups, photographs, schematics, progress, special and inspection reports, engineering notes, computations and training aids) shall be classified according to content. Guidance for classification shall be derived from the applicable Security Classification Guides, Government furnished equipment or data, or special instructions. Such material shall not contain contractor logos or similar identifiers which identify the specific contractor or team members."

2.2.10.8.2 Only include the information listed below if Item 10e(1) is "No" and Item 10f is "Yes:"

"Reference Item 10f: The Contractor Special Security Officers (CSSOs) shall coordinate with the DISA Security Division (D16) prior to subcontracting any portion of this contract.

a. All personnel requiring access to SAP information must be: U.S. citizens, have been granted a final Top Secret U.S. Government security clearance, have been approved as meeting DCID 1/14 criteria by a Government cognizant authority, and have been indoctrinated for the applicable SAP prior to being given access to such information generated or received under this contract. Immigrant aliens, interim cleared personnel or personnel holding a contractor granted CONFIDENTIAL clearance are not eligible for access to classified information released or generated under this contract without the expressed written permission of the Director, DISA (Security Division (D16), SSO.)

b. Contractor generated or Government furnished material may not be provided to the Defense Technical Information Center (DTIC). Contractor generated reports will bear the statement: ’Not Releasable to the Defense Technical Information Center per DOD Instruction 5230.24.’"

2.2.10.8.3 If Item 10f is "Yes," add the following in Item 13:

"Reference Items 10f and 11c: This contract will be performed in a facility approved through the DISA Security Division (D16) in accordance with applicable SAP security requirements. The CSO (DIS) may be relieved of security cognizance for the SAP by the DISA Security Division (D16) and/or the SAP Program Management Office (PMO) which will have responsibility for all SAP material or information released to the contractor under this contract."

2.2.10.8.4 If Items 10e(1) and/or 10f are "Yes," add: "Reference 10e(1) and/or 10f: Upon expiration of this contract, the contractor shall request disposition instructions for all classified and unclassified project material. The contractor may be directed to properly destroy the material or return it. If classified or unclassified project material is to be retained by the contractor, every effort should be taken to transfer it to a follow-on contract or similar effort, if applicable. This must be done, however, with KO approval. Unless written authorization by the KO to retain specific material for a specific period of time is received, the material shall be returned or destroyed as instructed. Any exception to security policy shall be referred to the CSO/DISA Security Division (D16) for coordination with the appropriate agencies and the contracting officer."

2.2.10.9 ITEM 10g, NATO INFORMATION:

This means information or documents belonging to and circulated by the North Atlantic Treaty Organization (NATO). Access to NATO requires a final U.S. Government clearance at the appropriate level. A representative of the Government will brief the Facility Security Officer (FSO), who in turn will brief other contractor personnel requiring access under the contract.
NOTE: To approve NATO access, include a statement such as: "Access up to and including NATO SECRET material will be required for reference only at the Government facility."

2.2.10.10 ITEM 10h, FOREIGN GOVERNMENT INFORMATION:

This item includes any foreign government information except NATO. Prior approval of the contracting activity is required before any subcontracting. Access to classified foreign government information requires a final U.S. Government clearance at the appropriate level.

2.2.10.11 ITEM 10i, LIMITED DISSEMINATION INFORMATION:

The use of the term "LIMDIS" has been removed from DOD 5200.1-R, Information Security Program, and will not be used within DISA/OMNCS contracts.

2.2.10.12 ITEM 10j, FOR OFFICIAL USE ONLY INFORMATION (FOUO):

This item is applicable only on a classified contract. When this item is marked "Yes," the contracting activity is responsible for providing the contractor with the safeguards and procedures necessary for the protection of the information. Specific guidance may be found in DOD 5400.7, Department of Defense Freedom of Information Act Program, Chapter 4, not the NISPOM. Also, insert the following statement in Item 14: "DOD Regulation 5400.7, DOD Freedom of Information Act Program." You must also provide them a copy of DOD Regulation 5400.7, DOD Freedom of Information Act Program.
NOTE: Non-DOD user agencies that use other terms that are similar to DOD FOUO are responsible for providing proper guidance to the contractor for their information requiring protection from public disclosure.

2.2.10.13 ITEM 10k, OTHER (Specify):

Use this item for any other information not included in Items 10a-10j. Specify the type of information and include any remarks needed in Item 13. If access is required to SAP information, state in Item 13 the unclassified name of the SAP program, the additional security requirements and measures needed, or state this information will be furnished under a separate cover. In Item 15, identify what oversight responsibility DIS is relieved of, and identify the office that has this oversight responsibility.

2.2.10.14 ACCESS REQUIREMENTS NOTE:

The access requirements listed above are included as part of the form because they are the most common situations that occur in classified contracts. If they do not apply to the contract requirements, indicate "No" for all of them,

add in Item 10k: "See Item 13," and include the appropriate statements in Item 13.

2.2.10.14.1 Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI):

Use the Item 10k block if the contract requires access to SIOP-ESI. Check the "Yes" block, and enter "SIOP-ESI." The following will be an attachment to the DD Form 254, incorporated into the DD Form 254, or be included in the Statement of Work (SOW):

"Reference 10k: This contract requires that specified contractor employees be granted access to Single Integrated Operational Plan - Extremely Sensitive Information (SIOP-ESI). Employees requiring SIOP-ESI access will be processed as follows:

a. The DISA COR will forward to the DISA Security Division (D16), via an Interoffice Memorandum (IM) a request to process certain employees of the company for SIOP-ESI access. The request will be marked with the appropriate markings (i.e., FOUO, Privacy Act Protected, etc.) and/or classified as may be required by SCG (i.e., justification). This request will contain the following:

(1) Name and SSAN of the employee(s).

(2) Company name, address, CAGE code, telephone number.

(3) Date and place of birth for employee(s).

(4) Citizenship of employee(s).

(5) Citizenship of employee’s spouse.

(6) SIOP-ESI Category required.

(7) Employee’s clearance level and date, investigation type and date.

(8) Inclusive dates SIOP access will be required.

(9) Contract number.

(10) Contract expiration date.

(11) Contract review date.

(12) Justification for requesting SIOP-ESI accesses.

b. The DISA Security Division (D16) will forward a letter to certify the need-to-know for SIOP-ESI access to the FSO at the company via DISA Form Letter 16.

c. When temporary access to SIOP-ESI has been approved by the Joint Chiefs of Staff, the DISA Security Division (D16) will forward this information to the FSO and authorize the employee to be briefed for access.

d. The FSO is responsible for notifying the DISA Security Division (D16) when the employee is transferred from one facility to another within the company, when the employee’s employment is terminated, when they resign, or have been transferred and do not require continued access.

e. The FSO is responsible for ensuring that the employees complete the required security forms for submission to DIS Clearance Office (DISCO) in a timely manner.

f. Information that an individual has been granted access to SIOP-ESI is unclassified."

2.2.11 ITEM 11, IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:

Mark these items "Yes" or "No" according to the requirements of each contract.
2.2.11.1 ITEM 11a, HAVE ACCESS TO CLASSIFIED ONLY AT ANOTHER CONTRACTOR’S FACILITY OR AT A GOVERNMENT FACILITY:

Note the word "only." This means that there will be no access to classified information at the contractor’s facility. The
contractor requires no safeguarding capability at its facility and Item 1b will be marked "N/A" or "None." If the "Yes" block is marked for this Item, add the following annotation in Item 13:

"Reference Item 11a: Contract performance is restricted to (enter the name and address of the contractor facility or Government activity). The using contractor or Government activity will provide security classification guidance for the performance of this contract."

2.2.11.2 ITEM 11b, RECEIVE CLASSIFIED DOCUMENTS ONLY:

Again, note the word "only." This means the contractor will receive classified documents and will not generate any classified information that will require detailed classification guidance. The classification markings shown on the documents received will provide the necessary security classification guidance. Add the following annotation in Item 13: "Reference Item 11b: Any classified information generated in performance of this contract shall be classified according to the markings on the source material. All classified information received is the property of the U.S. Government. The U.S. Government will be contacted at the expiration or termination of this contract for proper disposition instructions."

2.2.11.3 ITEM 11c, RECEIVE AND GENERATE CLASSIFIED INFORMATION:

This means the contractor is expected to receive and generate classified information (documents and/or hardware) and will require detailed SCG for performance of this contract.

2.2.11.3.1 If the "Yes" block is checked, detailed SCG must be provided to the contractor. The guidance may be included or referenced in Item 13, attached to the DD Form 254, forwarded under a separate cover, or included in the contract document itself. Statements, as appropriate, shall be included in Item 13 to direct the contractor to the guidance for the contract.

2.2.11.3.2 If the item is marked "Yes," the contractor will be required to prepare an Automated Information System Standard Practice Procedure (AIS/SPP) for their AIS operations and the system will require approval of the CSO/CSA in accordance with Chapter 8, NISPOM.

2.2.11.3.4 In all cases when this block is checked "Yes," add the statement: "Reference Item 11c: All classified information received or generated under this contract is the property of the U.S. Government. At the termination or expiration of this contract, the U.S. Government will be contacted for proper disposition instructions."

2.2.11.4 ITEM 11d, FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE:

If "Yes," include as much information as possible, (additional information can be added in Item 13), to indicate if Restricted or Closed Areas will be required. How much hardware is involved? How large? If more than 2 cubic feet of storage is required, contact the CSO to verify storage capability at the contractor facility.

2.2.11.5 ITEM 11e, PERFORM SERVICES ONLY:

If "Yes," add a statement in Item 13 explaining the services and to provide adequate and appropriate guidance. For service type contracts not covered, add any appropriate statement in Item 13 that explains why the contract is a classified contract and provide guidance as necessary to ensure protection of classified information.

2.2.11.5.1 Graphic Arts Services

Add the following statement in Item 13: "Reference Item 11e: Reproduction services only. The highest level of classification for this contract is (insert level). Classification markings on the material to be reproduced will provide the classification guidance necessary for the performance of this contract."

2.2.11.5.2 Engineering Services

Add the following statement in Item 13: "Reference Item 11e: Contract is for engineering services. Classification and markings on the material to be furnished will provide the classification guidance necessary for performance of this contract."

2.2.11.5.3 Equipment Maintenance Services

Add the following statement in Item 13: "Reference Item 11e: Contract is for equipment maintenance services on equipment which processes classified information. Actual knowledge, generation or production of classified information is not required for performance of this contract. Cleared personnel are required to perform this service because escorting personnel cannot preclude access to classified information. Any classification guidance needed will be provided by the using activity."

2.2.11.5.4 Guard Services

Add the following statement in Item 13: "Reference Item 11e: Contract is for Guard Services. Cleared personnel are required to perform this service."

2.2.11.6 ITEM 11f, HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S. PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES:

If "Yes," indicate exact location of overseas performance in Item 13. Item 14 may be "Yes" and should be completed as appropriate. A copy of the DD Form 254 must be provided to the Office of Industrial Security, International (OISI) or other U.S. activity responsible for overseas inspections. The appropriate addresses may be found in Appendix A of this handbook, or in Appendix A of DOD 5220.22-M, NISPOM.

2.2.11.7 ITEM 11g, BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR SECONDARY DISTRIBUTION CENTER:

A "Yes" in this item means the contractor is authorized to use the services of DTIC and will require the contractor to prepare and process DD Forms 1540 and 1541. The contracting activity will be involved in certifying need-to-know to DTIC. The COR must certify the need-to-know if this block is marked "Yes." Add the following statement to Item 13:

"Reference Item 11g:

a. The contractor must prepare and forward DD Forms 1540 and 1541 to the COR for authorization BEFORE the services may be requested.

b. Technical information on file at the Defense Technical Information Center (DTIC) will be made available to the contractor if the contractor requires such information. The contracting officer will certify the field of interest relating to the contract."

2.2.11.8 ITEM 11h, REQUIRE A COMSEC ACCOUNT:

If accountable COMSEC information will be provided to the contractor, mark the "Yes" box. If non-accountable COMSEC information is involved, mark the "No" box. Contact the DISA Security Division (D16) COMSEC Custodian, at Commercial (703) 681-0489 or DSN 761-0489 or 761-7950, before marking "Yes" on this item. If "Yes" is appropriate, add the statement referenced in Item 10a above. Item 11k, "Be authorized to use the Defense Courier Service" must also be marked "Yes" if the contractor has a need for a COMSEC account.

2.2.11.9 ITEM 11i, HAVE TEMPEST REQUIREMENTS:

TEMPEST requirements are in addition to the requirements of the NISPOM. If "Yes" in this item, Item 14 must also be "Yes" and the pertinent contract

clauses identified or the appropriate information added in Item 13. NOTE: Classified processing for the purpose of TEMPEST application is defined as SECRET or higher classification. CONFIDENTIAL processing is not considered for TEMPEST at a contractor's facility. The Procuring Contracting Officer (PCO) ensures potential TEMPEST situations related to performance of classified contracts are identified and evaluated. Contracts must include requirements for security countermeasures necessary to comply with National TEMPEST policy. The program/project manager identifies the necessary requirements to incorporate into the solicitation/contract and advises the PCO accordingly.

2.2.11.9.1 This item will be marked "Yes" only if processing classified information will be required at the contractor's facility. This includes AIS as well as word processing equipment. It does not apply if the contract is for maintenance service on AIS equipment or when the contractor will be performing the work at an UA or another cleared facility.

2.2.11.9.2 If this item is marked "Yes" and the contractor will be processing COLLATERAL level classified information at the contractor facility, an AIS/SSP for their AIS operations must be prepared and the system will require approval of the CSO in accordance with Chapter 8, NISPOM.

2.2.11.9.3 If "Yes," include the following statement in Item 13 or the Statement of Work, if the contractor will be processing COLLATERAL level classified information at the contractor facility:

2.2.11.9.3.1 "Reference 11i: The contractor shall not process classified information by electrical means prior to a DISA TEMPEST evaluation of the equipment/systems and facility, and written DISA certification that the facility meets DISA TEMPEST criteria. In order to expedite the DISA TEMPEST evaluation, the contractor shall provide a list of equipment, to include model number, which is associated with the processing of classified information. In addition, the estimated percentage of classified information processed, cable/conduit runs, a floor plan layout that depicts placement of equipment in relation to other rooms, equipment distances from walls or uncontrolled areas, and physical security being afforded the equipment both during processing and after hours. The above TEMPEST evaluation and DISA approval will not be required if previous DISA approval can be furnished and is no more than 2 years old. The existing approval must be for processing information at the same or higher level and at the same facility and items of equipment."

2.2.11.9.3.2 Include a statement in Item 13 of the DD Form 254 or in the Statement of Work similar to the following if SCI and/or SAP material is involved:

"Reference Items 11i and 10e(1) or 10f:

a. The contractor will not process classified information by electrical means prior to a TEMPEST evaluation of the equipment/systems and facility, and written DISA certification that the facility meets DISA TEMPEST criteria. In order to expedite the TEMPEST evaluation, the contractor shall provide a list and layout of equipment in accordance with DIAM 50-5, Volume I, Enclosure 13. The enclosure will include a floor plan layout that depicts placement of equipment in relation to other equipment, telephone lines and instruments, cable/conduit runs, etc. The drawing(s) are to show dimensions of rooms, physical relation to other rooms, equipment distances from walls or uncontrolled areas, and physical security being afforded the equipment both during processing and after hours.

b. Previous DISA approval may be furnished provided it is not more than 2 years old. The approval must be for processing information of the same or higher level security classification and for the same facility and items of equipment."

2.2.11.10 ITEM 11j, HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS:

OPSEC requirements are in addition to the normal handling procedures and requirements of the NISPOM. There is NO specific OPSEC procedures or requirements listed in the NISPOM. If "Yes" in this item, Item 14 must also be "Yes" and the pertinent contract clauses identified or appropriate information added in Item 13. The contracting activity will be involved in approving OPSEC requirements for subcontracts. Contact the DISA Security Division (D16), at Commercial (703) 681-1331 or DSN 761-1331, and the CSA for further information. Include the following statements in Item 14: "OPSEC requirements apply. The contractor will comply with special OPSEC requirements contained in the contract or addendum thereto." CORs will comply with DOD Directive 5205.2, DOD Operations Security (OPSEC) Program, the NISPOM, and ISR.

2.2.11.11 ITEM 11k, BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE (DCS):

This item authorizes the contractor to use the services of DCS. If this item is marked "Yes," the COR requests services from the Commander, DCS, ATTN: Operations Division, Fort George G. Meade, MD 20755-5370. Only certain classified information qualifies for shipment by DCS. It is the responsibility of the contracting activity to comply with DCS policy and procedures. This item must be marked "Yes" if Item 11h "Require a COMSEC Account" is marked "Yes."

2.2.11.12 ITEM 11l, OTHER (SPECIFY):

Use this item to add any additional performance requirements not covered above. Item 13 should be appropriately annotated to provide any necessary remarks.

2.2.11.13 NOTE:

The performance requirements listed above are included as part of the form because they are common situations that occur in classified contracts. If they are not applicable to the contract requirements, indicate "No" for all of them, add in Item 11l: "See Item 13," and include appropriate statements in Item 13.

2.2.12 ITEM 12, PUBLIC RELEASE:

The contractor obtains contracting activity approval before releasing any information received or generated under the contract, except certain types of information authorized by the NISPOM, Section 5-5. If desired or required by the nature of the contract, mark the "Through" box and add the address of the OCA for the information. If multiple sources are used to classify the information required under this contract, use your address.

2.2.12.1 For Unclassified and collateral information: The contractor is responsible for obtaining the approval of the contracting activity prior to release of any information received or generated under this contract, except certain types of information authorized by the NISPOM, Section 5-5. Complete this item as required by internal agency directives to direct the contractor to the office in the UA that should receive proposed public releases.

2.2.12.2 If access to SCI or a SAP s required (Item 10(e)1 or 10f is "Yes) include the following: "Public release of SCI/SAP is not authorized."

2.2.13 ITEM 13, SECURITY GUIDANCE:

This is the most important part of the entire DD Form 254. Reference all attachments in this block. Make all of your instructions clear. If you fill this block, use an attachment(s). If the contractor does not classify the material correctly, it can directly affect national security. Use this item to identify applicable guides, provide narrative guidance which identifies the specific information to be classified, to provide appropriate downgrading or declassification instructions, to provide any special instructions, explanations, comments or statements required for information to clarify any other items identified in the DD Form 254. Ask yourself these questions:

What classified information does the contractor need to perform this contract?
What guidance does the contractor need to protect the classified information?
Is there existing security classification guidance for the program/project?

What portion of the guide applies to the contract? All or part? Are there other guides that may provide guidance to assist the contractor?

Will classified hardware be furnished to or generated by the contractor? What information makes the hardware classified? Does hardware being generated require classification? At what stage in production does it become classified?

What unique characteristics are involved that need protection? Are there design features that require protection? What technical information requires protection? What breakthroughs would be significant if achieved in a Research and Development effort? Is there some performance limitations that require protection?

2.2.13.1 These are merely some of the questions to ask when preparing guidance for a contract. Put yourself in the contractor’s place and try to determine what guidance is needed to properly protect the classified information provided under this contract.

2.2.13.2 Enter program/project manager’s name, title, organization, telephone number and signature and contract expiration date in this item.

2.2.13.3 Each contract is unique in its performance requirements. Give reasons for the classification. Write the guidance in plain English. Use additional pages as necessary to expand or explain the guidance. Additional pages will contain a heading identifying the contractor’s name, contract number/RFQ/RFP/IFB, contract date, and revision number.

2.2.13.4 The DD Form 254, with its attachments and incorporated references, is the only authorized means for providing SCG to a contractor. It should be written as specifically as possible and should include only that information pertaining to the issued contract.

2.2.13.5 The requirements from the NISPOM or its supplements should not be extracted and included in a DD Form 254; the NISPOM provides safeguarding requirements and procedures for classified information, not SCG.

2.2.13.6 It should not contain references to internal agency directives and instructions. If such documents provide guidance applicable to the contract, the pertinent portions should be extracted and provided as attachments. Any and all documents referenced or cited in Item 13 should be provided to the contractor, either as attachments, or under separate cover if they are classified.

2.2.13.7 It is a difficult task to prepare a SCG that covers all of the performance requirements of a classified contract. It is an even more difficult task to prepare guidance that can be understood and implemented by the contractor. Encourage the contractor to assist in the preparation of the SCG, if at all possible, and to provide comments and/or recommendations for changes in the SCG that have been provided. Only through effective communication with the contractor can you achieve a SCG that is understandable and will ensure the proper classification and protection of the information generated in the performance of the contract.

2.2.13.8 General Information: The following statements will always be added to Item 13:

"All classified visit requests by contractors shall be forwarded to the COR for approval and need-to-know certification before being sent to the facility to be visited.

The COR must be notified and approve the receipt and/or generation of classified information under this contract.

All classified information received and/or generated under this contract is the property of the U.S. Government regardless of proprietary claims. Upon completion or termination of this
contract, the U.S. Government will be contacted for destruction or disposition instructions."

2.2.14 ITEM 14, ADDITIONAL SECURITY REQUIREMENTS:

This item applies anytime there are security requirements imposed on the contractor, in addition to the requirements of the NISPOM or its supplements. "Yes" in this item requires the contracting activity to incorporate the additional requirements into the contract document itself or reference in Item 13. Attendant costs incurred due to additional security requirements are subject to negotiation by and reimbursement to the contractor and
are the responsibility of the contracting activity imposing the additional security requirements. You must provide a copy of the additional security requirements to the CSO. Also, you must list any additional regulations, instructions, etc., you are imposing on the contractor. For example, if you identify the need for access to Non-SCI Intelligence Information, you must put "Director of Central Intelligence Directive (DCID) 1/7, Security Controls on the Dissemination of Intelligence Information, 12 April 1995."

2.2.15 ITEM 15, INSPECTION INFORMATION:

This item applies when the CSO is relieved of inspection responsibility in whole or in part. A "Yes" in this item requires the contracting activity to provide information on the specific areas "carved-out" from DIS cognizance and to identify the activity responsible for inspection. A copy of the DD Form 254 must be provided to the CSO and the DISA Security Division (D16).

2.2.16 ITEM 16, CERTIFICATION AND SIGNATURE:

Item 16 shall contain the name, title, telephone number, address and signature of the PCO or KO certifying that the requirements are complete and adequate for performance of the classified effort.

2.2.17 ITEM 17, REQUIRED DISTRIBUTION:

The DD Form 254 is a contractual document and should be distributed with the contract document to all addressees by the PCO. If the Statement of Work (SOW) is a separate document, it will be sent with the DD Form 254 through the DISA Security Division (D16) during the coordination phase. It is essential that the DD Form 254 be distributed, as a minimum, to those shown in this item and those listed on the DISA Form 173, DISA Contract Points of Contact for Administration of DD 254.

2.2.17.1 Item 17f, OTHERS AS NECESSARY
This item will always be marked with an "X," and the following instruction typed next to it: "DISA Industrial Security"

APPENDIX A: DISA FORM 173, DISA CONTRACT POINTS OF CONTACT FOR ADMINISTRATION OF DD 254

1.1 This form will be attached to ALL DISA DD Forms 254. The KO and the COR must complete Blocks 1 through 14. A new form will be completed whenever there is a change in KO/COR and the form distributed to all recipients of the DD Form 254.

1.2 The DISA Security Programs and Oversight Branch (D161) will not initial for review if the DD Form 173 has not been signed by the COR. This is to ensure the COR has seen the changes to the DD Form 254.

1.3 Add the following to Item 15 of DISA Form 173:

Required Distribution:
(Place an "X" in front of each office that must coordinate on this DD Form 254.)

__ Industrial Security Program Manager
Commercial (703) 681-4468 or DSN 761-4468

__ DISA Security Operations Division (D162).
Commercial (703) 681-7990 or DSN 681-7990

SCI Access(es) _____; Billets _____; Documents _____.
SAP (SAP CCO) Access(es) _____; Billets ____; Docs _____.
COMSEC Account Number _____; STU III _____.
Defense Courier Service (DCS) Acct _____.

__ SIOP-ESI Information COMM (703) 681-1349 or DSN 761-1349

__ OPSEC COMM (703) 681-7990 or DSN 761-7990

__ Collateral TEMPEST Information - Include in distribution on all DISA DD Forms 254 requiring classified automated data processing or word processing (including electric typewriters) EXCEPT those with SCI or SAP requirements.

APPENDIX B: BASIC COR RESPONSIBILITIES

B.1 The COR responsible for the contract will accomplish the following:

B.1.1 Route all DD Forms 254 through the DISA Security Division (D16) for coordination.

B.1.2 Ensure a copy of the signed DD Form 254 and DISA Form 173 are forwarded to D16.

B.1.3 Forward copies of DD Forms 254 signed by prime contractors for subcontracting to D16.

B.1.4 Forward the letter of biennial review to D16. D16 will forward a copy to the CSO.

B.1.5 Authorize all releases of classified information to contractors. The COR will verify the classified information is needed in performance of the contract. Use DISA Form 621: Transmittal Record, (Figure 2) for this purpose. Ensure a copy is sent to the KO for inclusion in the main contract file.

B.1.6 Assist in the close out of the contract. Specifically, forward to D16 the following:

B.1.6.1 Date that the contract is officially completed.

B.1.6.2 Verification that all classified material received or generated under the contract by the contractor has been destroyed or returned to DISA.

B.1.6.3 Requests to retain any or all classified material generated under the contract, along with approval or disapproval.

B.1.6.4 Notification of classified material being transferred to a follow-on contract.

B.1.6.5 The above information, except Item 3, should be forwarded to D16 in one single report, as soon as possible, but not more than 1 year after completion date of the contract. Item 3 may be forwarded no later than 2 years after completion of the contract.

APPENDIX C: AUTOMATED DATA PROCESSING POSITION SENSITIVITY DESIGNATIONS

C.1. All positions within the Defense Information Systems Agency, Office of the Manager, National Communications System (DISA/OMNCS), must be identified with their level of Automated Data Processing (ADP) sensitivity in accordance with
DOD 5200.2-R, Personnel Security Program Regulation (reference "f"). This includes all positions occupied by contractors working for the Agency.

C.2. The minimum ADP position sensitivity designation level for all positions within DISA/OMNCS is "non-critical sensitive." The minimum investigation required is a National Agency Check Plus Written Inquiries (NACI).

C.3. ADP sensitivity designations must be included on all contracts, including those contracts that deal with classified information. Table 1, Position Sensitivity Designation Descriptions (Enclosure 1), identifies the correct definitions for ADP position sensitivity designations as designated in reference.

C.4. The contracts/solicitations must include a statement that all DISA/OMNCS positions must be designated with their ADP Sensitivity, and what investigations will be required. These descriptions (Appendices C and D) should be included in "Section H" of the contract/solicitation.

C.5. The Statement of Work (SOW) must include a clause identifying all applicable regulations. A sample SOW clause is included in Table 2, Position Sensitivity SOW Clause (Appendix D, Table 2).

C.6. All investigation paperwork that is submitted must be accompanied by a letter from the COR identifying the contract is a valid DISA/OMNCS contract.

APPENDIX D: AUTOMATED DATA PROCESSING (ADP) POSITION DESCRIPTIONS AND INVESTIGATION REQUIREMENTS

D.1. Critical-Sensitive Positions (ADP-I positions):

Those positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain. ADP-I designated positions require a Single Scope Background Investigation (SSBI).

D.2. Non-critical-Sensitive Positions (ADP-II positions):

Those positions in which the incumbent is responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP-I category to ensure the integrity of the system. ADP-II designated positions require a DOD National Agency Check Plus Written Inquiries (DNACI)/National Agency Check Plus Written Inquiries (NACI).

D.3. Non-sensitive Positions (ADP-III positions):

All other positions involved in computer activities. In establishing the categories of positions, other factors may enter into the determination, pertaining to placement in higher or lower categories based on the Agency’s judgment as to the unique characteristics of the system or the safeguards protecting the system. ADP-III designated positions require a National Agency Check (NAC) or Entrance National Agency Check (ENTNAC). There are NO Non-sensitive positions within DISA.

TABLE 1. POSITION SENSITIVITY DESIGNATION DESCRIPTIONS

Category CriteriaADP-I
Responsibility for the development and administration of Agency computer security programs, and also including direction and control of risk analysis and/or threat assessment. Significant involvement in life-critical or mission-critical systems.
Responsibility for the preparation or approval of data for input into a system which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.
Relatively high risk assignments associated with or directly involving the accounting, disbursement,(1) dollar amounts of $10 million per year or greater, or (2) lesser amounts of the activities of the individual are not subject to technical review by higher authority in the ADP-I category to insure system integrity.

Positions involving major responsibility for the direction planing, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.

Other positions as designated by the Agency Head that involve relatively high risk for effecting grave damage or realizing significant personal gain.

ADP-II
Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the ADP-1 category. It includes, but is not limited to:

(1) access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974 (reference m), and Government-developed privileged information involving the award of contracts;

(2) accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than $10 million per year. Other positions are designated by the Agency Head that involve a degree of access to a system that creates a significant potential for damage or personal gain less than ADP-I positions.

ADP-III
All other positions involved in Federal computer activities.

APPENDIX E: ADP POSITION SENSITIVITY DESIGNATION STATEMENT OF WORK REQUIREMENTS

E.1. Position Sensitivity:

To ensure that contractor personnel have been properly checked or investigated, the system owner must determine the sensitivity of the positions to which the contractor personnel are assigned and the level of investigation required. Sensitivity of the information to be processed by the delivered system, threats to the environment, and existing computer security safeguards are to be considered when determining position sensitivity. For example, in a system processing highly sensitive information, a lead system programmer position, with unlimited system privileges, would be considered ADP-I. A data entry position with no privileges other than entering information into the computer under strict technical control, would be rated ADP-III. Table 2, Position Sensitivity SOW clause, may be used to define and justify the personnel security requirement in SOWs. List positions regarded as sensitive, assign the appropriate personnel security designation and list the investigative requirement. For example: Supervisory Computer Operator: ADP-I w/SSBI; Systems Analyst: ADP-II w/NACI; Systems Programmer: ADP-II w/NACI; Lead Systems Programmer: ADP-I w/SSBI.
TABLE 2. POSITION SENSITIVITY SOW CLAUSE

"DOD 5200.2-R, DOD Personnel Security Program, requires DOD military and civilian personnel, as well as DOD consultant and contractor personnel, who perform work on sensitive automated information systems (ISs), to be assigned to positions which are designated at one of two sensitivity levels (ADP-I, ADP-II). These designations equate to Critical Sensitive, Non-critical Sensitive. The contractor will assure that individuals assigned to the following sensitive positions, as determined by the Government, have completed the appropriate forms.
The required investigation will be completed prior to the assignment of individuals to sensitive duties associated with the position. The contractor will forward their employee clearance information (completed SF 85P, Questionnaire for Positions of Public Trust, and two DD Forms 258 (Fingerprint cards) to: DISA Security Division (D16); ATTN: Personnel Security (D162); 5111 Leesburg Pike, Suite 100; Falls Church, VA 22041-3206.
DISA retains the right to request removal of contractor personnel, regardless of prior clearance or adjudication status, whose actions, while assigned to this contract, clearly conflict with the interests of the Government. The reason for removal will be fully documented in writing by the Contracting Officer. When and if such removal occurs, the contractor will within [specify number of days] working days assign qualified personnel to any vacancy(ies) thus created."

APPENDIX F: OPERATIONAL AREAS OF DIS COGNIZANT SECURITY OFFICES
NORTHEAST REGION
The Northeast Region, New England Sector includes: Puerto Rico and the states of Connecticut, Maine, Massachusetts, New Hampshire, New York, Rhode Island, Vermont and the following ZIP codes in New Jersey:

07001-07699
07801-07999

The Northeast Region, Mid-Atlantic Sector, includes: the states of Delaware, New Jersey (less the ZIP codes listed above), Pennsylvania, Ohio, West Virginia, and the following ZIP codes in Maryland:
215__ all of 217__ except
23,37, 38, 65 and 97
21048, 80, 88
21107,55, 57219__
210__
212__
216__CAPITAL AREA
The Capital Area includes: the state of Virginia, Washington D.C., and the following ZIP codes in Maryland:
20814-17
20832-33
20842
20850-5520861
20866
20871
20874-7920895
20901-06
20910
20912206__

207__
21401
21403-04SOUTHEAST REGION
The Southeast Region includes: the states of Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, South Carolina, Tennessee, and the following ZIP codes in eastern Texas:
75501
75505
7557075662
75671
75755CENTRAL REGION

The Central Region, Southwest Sector includes: the states of Arizona, Colorado, New Mexico, Oklahoma, and Texas (less the ZIP codes listed above).

The Central Region, Midwest Sector includes: the states of Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, Wisconsin, and Cheyenne, Wyoming.
PACIFIC REGION
The Pacific Region, Northern Sector includes: the states of Idaho, Montana, Oregon, Washington, Wyoming (except for Cheyenne), Utah, and the following ZIP codes in California:

•93612 •93706 •93923 •93940 •94022 •94042 •94086 •94303 •94535 •94537 •94544 •94560 •94587 •95006 •95008 •95014 •95020 •95023 •95030 •95037 •95050 •95060 •95070 •95101 •95134 •95360 •94002 •94010 •94025 •94030 •94044 •94066 •94070 •94101 •94302-06 •94402 •94501 •94510 •94513 •94520 •94524 •94530 •94533/46 •94549/50 •94554 •94558 •94563 •94565 •94566 •94570 •94574/77 •94583 •94585 •94596 •94599 •94608 •94615 •94701 •94708 •94802 •94952 •95208 •95240 •95336 •95338 •95367 •95376 •95402-07 •95501 •95608 •95611 •95616/19 •95630 •95648 •95660 •95670 •95673/75/87 •95695 •95741 •95813 •95926 •96067 •96099 •96137

The Pacific Region, Southern Sector includes: The states of Alaska, California (less the ZIP codes listed above), Hawaii, and Nevada.

APPENDIX G: ADDRESSES AND TELEPHONE NUMBERS

Northeast Region, DIS
New England Sector
Barnes Building 1040
495 Summer Street
Boston, MA 02210-2192
COMM: (617) 451-4914
DSN: 955-4914
FAX: (617) 451-3052/4929

Central Region, DIS
Southwest Sector
106 Decker Court, Suite 200
Irving, TX 75062-2795
COMM: (214) 717-5228
FAX: (214) 717-0268

Pacific Region, DIS
Southern Sector
3605 Long Beach Blvd, Suite 405
Long Beach, CA 90807-4013
COMM: (310) 595-7251
FAX: (310) 595-5584

Capital Area, DIS
Hoffman Building
2641 Eisenhower Avenue
Alexandria, VA 22331-1000
COMM: (703) 325-9634
DSN: 221-9634
FAX: (703) 325-0792

Northeast Region, DIS
Mid-Atlantic Sector
Kings Highway North
Cherry Hill, NJ 08034-1908
COMM: (609) 482-6505
DSN: 444-4030
FAX: (609) 482-0286

Central Region, DIS
Midwest Sector
610 S. Canal Street
Room 908
Chicago, IL 60607-4599
COMM: (312) 886-2436
FAX: (312) 353-1538

Pacific Region, DIS
Northern Sector
Building 35, Room 114
The Presidio
San Francisco, CA 94129-7700
COMM: (415) 561-5608
FAX: (415) 561-2125

Southeast Region, DIS

2300 Lake Park Drive
Suite 250
Smyrna, GA 30080-7606
COMM: (404) 432-0826
DSN: 697-6785
FAX: (404) 801-3300

APPENDIX H: OTHER INDUSTRIAL SECURITY ADDRESSES

OISI-Europe (OISI-E)
PSC 79 Box 003
APO AE 09724
COMM: 011-322-725-0884
FAX: 011-322-725-0116
SECURE: 9-022/322/720-9015

OISI-Far East (OISI-FE)
Unit 45005
APO AP 96343-5005
COMM: 011-81-3117-63-3619
FAX: 011-81-3117-63-3622
DSN: 263-3619

OISI-FE (Mannheim)
HQ USAMC-E
Unit 29331
APO AE 09724
COMM: 011-49621-472582
FAX: 011-49621-815517

OISI-CASA (Central
and South America)
DIS, Industrial Security
Field Office(S41ME)
1600 Sarno Road, Suite 201
Melbourne, FL 32935-4992
COMM: (407) 255-5185
FAX: (407) 255-5192

DISCO
P.O. 2499
Columbus, OH 43216-5006
COMM: (614) 692-2133
DSN: 850-2133
FAX: (614) 692-3663/5263

Verification of Facility Clearance and Safeguarding

Defense Industrial Security Clearance Office (DISCO)
ATTN: Central Verification Activity (CVA)
P.O. Box 2499
Columbus, OH 433216-5006
COMM: (614) 692-3688 or 2087
FAX: (614) 692-3669
Back to Top | Deskbook Page

Mission | Organization Chart | POCs | Acquisition | Logistics | Real Estate & Facilities
DISA Home Page | Products & Services Catalog | Procure & Log Home Page | Site Map

crossv@ncr.disa.mil, 10/9/97 jlw